RESUMEN – TRABAJO DE GRADO

AUTORES	**PEDRO LUIS SÁNCHEZ GONZÁLEZ**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION AUDITORIA DE SISTEMAS**
DIRECTOR	**JOSE LUIS MARTINEZ MENDOZA**
TÍTULO DE LA TESIS	**DISEÑO DE UN PLAN DE MEJORAMIENTO PARA GARANTIZAR LA CONFIDENCIALIDAD DE LA INFORMACIÓN DE LA EMPRESA ECORED S.A.S**

RESUMEN
(70 palabras aproximadamente)

LA EMPRESA ECOLÓGICA DE RECICLAJE Y DIGITALIZACIÓN DE ARCHIVOS (ECORED S.A.S) ESTÁ DEDICADA EN LA RECUPERACIÓN, RECOLECCIÓN Y TRANSFORMACIÓN DE MATERIAL RECICLADO PARA SER REUTILIZADO Y GENERAR PRODUCCIÓN DE PAPEL, CON SU GRAN COMPROMISO CON EL MEDIO AMBIENTE Y LA SOCIEDAD, TAMBIÉN ORGANIZA Y DIGITALIZA ARCHIVOS A TRAVÉS DE ESTRATEGIAS DIRIGIDAS A LA COMUNIDAD Y A LOS GRUPOS EMPRESARIALES, GENERANDO CONCIENCIA SOBRE LA IMPORTANCIA DE CONSERVAR EL PLANETA. ESTA ORGANIZACIÓN PRESENTA LA NECESIDAD DE CONTAR CON UN PLAN ESTRATÉGICO QUE PERMITA MEJORAR LA SEGURIDAD DE LA CONFIDENCIALIDAD Y QUE CONTRIBUYA A LA CONSECUCIÓN DE LOS OBJETIVOS DEL NEGOCIO APOYADOS EFICIENTEMENTE CON EL RECICLAJE Y MEDIO AMBIENTE.

CARACTERÍSTICAS

PÁGINAS: 60	PLANOS: 0	ILUSTRACIONES: 32	CD-ROM: 1

DISEÑO DE UN PLAN DE MEJORAMIENTO PARA GARANTIZAR LA CONFIDENCIALIDAD DE LA INFORMACIÓN DE LA EMPRESA ECORED S.A.S

PEDRO LUIS SÁNCHEZ GONZÁLEZ

850184

DIRECTOR

JOSE LUIS MARTINEZ MENDOZA

INGENIERO DE SISTEMAS

ESPECIALISTA EN AUDITORÍA DE SISTEMAS

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACION AUDITORIA DE SISTEMAS

Ocaña, Colombia **Noviembre, de 2019**

Índice

Lista de Tablas

Lista de Figuras

Capítulo 1. Diseño De Un Plan De Mejoramiento Para Garantizar La Confidencialidad De La Información De La Empresa Ecored S.A.S

1.1 Planteamiento del problema

La razón principal de diseñar un plan de mejoramiento para fortalecer la confidencialidad de la información de la empresa ECORED S.A.S es la necesidad que surgió después de que la empresa fue víctima de un robo de datos, por parte de personas que aún se desconoce sus paraderos. Debemos tener en cuenta que toda empresa está en la obligación jurídica de proteger los datos que les deposita sus clientes.

Uno de los principales beneficios es que se deriva la mayor protección de la privacidad, ya que todos los consumidores tienen una preocupación especial por la privacidad de su información personal, y especialmente cuando se refieren a su domicilio y número de celular.

La empresa está en la obligación de dar solución informática y desarrollar servicios de monitoreo y un plan de auditorías en seguridad informática, y dicha solución se debe dar de carácter permanente para que así la empresa se mantenga segura de posibles desvíos de datos.

1.2 Formulación del problema

¿Puede un plan de mejoramiento fortalecer la confidencialidad de la información de la empresa ECORED S.A.S y así prevenir daños e interferencias en los datos?

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un plan de mejoramiento para garantizar la confidencialidad de la información de la empresa ECORED S.A.S

1.3.2 Objetivos específicos

- Realizar un diagnóstico de la situación actual de seguridad de la información.
- Determinar el grado de importancia que tiene para la empresa la protección de datos, tales como: financieros, base de datos de clientes e información TI (ordenadores y equipos de telecomunicación).
- Elaborar un PETI, y determinar qué tipo de software se le podría aplicar a la empresa.

1.4 Justificación

A medida que las empresas van avanzando en este mundo tan competitivo, el proceso de investigación y desarrollo propio de las organizaciones se genera conocimiento que tiene el potencial de generar valor agregado para la empresa, pero revelar dicho conocimiento sin haber tomado las medidas para protegerlo puede causar pérdidas de recursos y oportunidades de negocio. Aun así, existen empresas que deciden mantener confidencialidad absoluta para que no surjan problemas, y eso está bien, porque dicha confidencialidad es importante en todas las

compañías, especialmente para las pequeñas empresas y emprendedores que generalmente subcontratan servicios de terceros. Por lo tanto, es aconsejable que la empresa celebre acuerdos de confidencialidad con quienes participen en el proceso creativo y se obliguen a mantener la información en secreto hasta que sea prudente publicarla.

En Colombia existen empresas que son ignorantes en el tema de la seguridad de la información y esas empresas no pueden visualizar un ataque o intromisión a sus sistemas y tampoco, las deficiencias que estructuralmente posee para salvaguardar sus equipos y la información contenida en ellos.

La empresa Ecológica de reciclaje y digitalización de archivos (ECORED S.A.S) está dedicada en la recuperación, recolección y transformación de material reciclado para ser reutilizado y generar producción de papel, con su gran compromiso con el medio ambiente y la sociedad, también organiza y digitaliza archivos a través de estrategias dirigidas a la comunidad y a los grupos empresariales, generando conciencia sobre la importancia de conservar el planeta. Esta organización presenta la necesidad de contar con un plan estratégico que permita mejorar la seguridad de la confidencialidad y que contribuya a la consecución de los objetivos del negocio apoyados eficientemente con el reciclaje y medio ambiente.

1.5 Delimitación

1.5.1 Delimitación espacial o geográfica. El proyecto se realizará en la empresa ECORED S.A.S que está ubicado en el municipio de Valledupar.

1.5.2 Delimitación temporal. El proyecto se desarrollará durante 10 meses, en los cuales se llevarán a cabo cada una de las actividades propuestas.

1.5.3 Delimitación Contextual

Reseña histórica de Valledupar

Valledupar, también llamada Ciudad de los Santos Reyes del Valle de Upar, es un municipio colombiano, capital del departamento del Cesar. Es la cabecera del municipio homónimo, el cual tiene una extensión de 4493 km2, 493 342 habitantes y junto a su área metropolitana reúne 677 9413 habitantes; está conformado por 25 corregimientos y 102 veredas.

Está ubicada al nororiente de la Costa Atlántica colombiana, a orillas del río Guata purí, en el valle del río Cesar formado por la Sierra Nevada de Santa Marta al occidente y la serranía del Perijá al oriente.

(Wikipedia, 2000)La ciudad es un importante centro para la producción agrícola, agroindustrial y ganadera en la región comprendida entre el norte del departamento del Cesar y el sur del departamento de La Guajira, en el punto intermedio de las dos cuencas de explotación carbonífera más grandes del país: Cerrejón al norte y el complejo minero operado por Glencor La Loma-La Jagua al sur. También es uno de los principales epicentros musicales, culturales y folclóricos de Colombia por ser la cuna del vallenato, género musical de mayor popularidad en el país y actualmente símbolo de la música colombiana. Anualmente atrae a miles de visitantes de

Colombia y del exterior durante el Festival de la Leyenda Vallenata, máximo evento del vallenato.

Reseña histórica de la empresa ECORED S.A.S

ECORED, es una empresa dedicada a la recuperación, recolección, transformación del material reciclaje para su reutilización y la producción de papel, comprometida con el medio ambiente y la sociedad, que busca mitigar el uso irracional de recursos naturales renovables, como son; el agua, la energía y la madera (arboles), a través de gestión documental en la comunidad y grupos empresariales.

Esta empresa nació por la necesidad de crear conciencia del medio ambiente, y de reciclaje a toda la comunidad en general, además de diseñar proyectos empresariales que ayudan a la organización de archivos, disposición final de los mismos, reducción de los niveles de utilización del papel y digitalización de la información.

La idea nace de un grupo de amigos (ingeniero ambiental, ingeniero de sistema y auditor de calidad) que quieren contribuir con la conservación del planeta, viendo en el reciclaje, la reutilización y la concientización de las personas y empresas una oportunidad de cambio.

(ECORED , 2006)

MISIÓN

Somos una empresa ecológica de reciclaje y digitalización de archivos, comprometidas con el medio ambiente, que obtiene material reciclaje para su reutilización y producción de nuevos productos, organiza y digitaliza archivos a través de estrategias dirigidas a la comunidad y a los grupos empresariales, generando conciencia con sobre la importancia de conservar el planeta, trabajando con amor y compromiso.

VISIÓN

Ser en el 2018 una empresa líder en la recolección y producción de productos a partir de material reciclado, la digitalización de información y la reducción del papel con gran presencia a nivel local, nacional e internacional.

VALORES

CONFIDENCIALIDAD: La reserva y confidencialidad de la información en el material reciclado es el principal objetivo con nuestros clientes.

HONESTIDAD: Actuando con honestidad hemos logrado construir la confianza de nuestros clientes, empleados y aliados, lo que nos permite garantizar la calidad en el cumplimiento de nuestros servicios.

AMOR: El amor por lo que hacemos y las ganas de contribuir con la creación perfecta de Dios nos lleva a trabajar juntos para lograr nuestros objetivos.

COMPROMISO: Orden, puntualidad y responsabilidad son características propias del compromiso de nuestro equipo con cada uno de nuestros clientes y proyectos.

Capítulo 2. Marco referencial

2.1 Marco histórico

En la empresa ECORED S.A.S nunca se ha realizado un diseño de plan de mejoramiento para el fortalecimiento de la confidencialidad de la información.

2.1.1 Mundial

Seguridad informática

Sapsi toma una visión integral de la empresa, ocupándose en todo momento de que la compañía pueda realizar sus negocios con la seguridad de que los sistemas informáticos y la infraestructura de apoyo le responderán.

En un ámbito comercial totalmente informatizado es indispensable que la empresa cuente con un respaldo que le permita operar con la tranquilidad y seguridad necesaria para el buen desarrollo de sus operaciones.

* Copias de Seguridad Remotas.
* Monitorización Sistemas.
* Tests de penetración y auditorías persistentes de Sistemas.
* Sistemas Antiespionaje.

* Servicio de Localización de Intrusos.

* Sistemas de Seguridad en Cloud avanzados.

SBCP – Plan de Continuidad de Negocio

Un **Plan de Continuidad de Negocio** (o BCP) es necesario para el éxito duradero de toda organización. Tener implantado un BCP no sólo **protege la información** crítica de su negocio contra una posible destrucción total, sino que permite afinar los procesos de su negocio y así poder volver a la normalidad en caso de disrupción parcial o total de las operaciones diarias.

La solución **SBCP (Sapsi Business Continuity Planning)** está basada en buenas prácticas mundialmente reconocidas y en normas internacionalmente aprobadas y su base origina en la gestión de riesgos. La Gestión de **Continuidad de Negocio** se arraiga en un proceso continuo empezando por un buen conocimiento del entorno de nuestros clientes con el objetivo de que la continuidad forme parte de la propia estrategia de la organización.

El proceso en su totalidad incluye las siguientes fases:

- Obtener un conocimiento de su negocio a través de la iniciación del proyecto.
- Realizar un **análisis de impacto** cuyo objetivo es determinar los procesos críticos de la empresa, evaluar sus impactos económicos y operacionales sobre el negocio en caso de no disponer de los recursos humanos, logísticos o tecnológicos para ejecutarlos además de establecer un orden de prioridad de recuperación de dichos procesos.

- Realizar un **análisis de riesgos** en el que se valoran los riesgos a los que están expuestos su negocio y más específicamente los procesos críticos identificados en la fase anterior dejando como opciones: eliminar, mitigar o asumir los riesgos valorados.

- Desarrollar unas **estrategias de continuidad** y valorarlas hasta llegar a un equilibrio entre los gastos incurridos, los riesgos a mitigar y los beneficios económicos aportados.

- Documentar los procedimientos a seguir según la estrategia adoptada. Los procedimientos incluyen la planificación de los recursos, la logística y la tecnología necesaria para recuperar los servicios mínimos de su empresa.

- Probar las **soluciones de recuperación** y realizar ejercicios basados en el Plan para asegurar su buen funcionamiento y para poder actualizar los puntos débiles encontrados durante esta fase.

- Sensibilización y formación de la plantilla al BCP y la importancia que éste tiene para su negocio.

Dentro de un **Plan de Continuidad de Negocio** se pueden incluir (de manera sucesiva o exclusiva):

- **El Plan de Recuperación de Desastres (DRP)** tecnológicos cuyo objetivo es proporcionar una solución tecnológica en caso de fallo de los sistemas sea a través de proveedores externos o desarrollando una solución interna.

- **El Plan de Continuidad de Operaciones (COOP)** que consiste en asegurar la continuidad de las operaciones a través de la contratación de servicios logísticos adecuados.

(Sapsi, 2003)

2.1.2 Nacional. "En Colombia una de las empresas que presta servicios de protección de información es Colombia Digital, tiene servicios en la nube que consiste en protección con estrategias de ciberseguridad." (Digital, 2010)

Los servicios en la Nube son cada día más usados y requeridos por compañías de todos los tamaños en nuestro país. Para conocer de cerca los beneficios y desafíos en ciberseguridad, de esta tecnología disruptiva, varios expertos compartieron sus experiencias y conocimientos acerca del tema.

"Existe la legislación que protege la información, fue creado gracias al Ministerio de Interior y de Justicia, Ministerio TIC, Ministerio de Defensa Nacional, Departamento Administrativo de Seguridad, Fiscalía General de la Nación y Juzgados Penales"

(interior)

2.2 Antecedentes

Como lo afirma el ministerio del interior (2010) “Según el acuerdo con la expedición del Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 del 2015 del sector de Tecnologías de la información y las Comunicaciones, la ESAP trabaja permanentemente en pos de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información –MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.” (interior, pág. 12)

La seguridad de la información consiste en preservar la confidencialidad de la misma, así como su integridad y disponibilidad. Esto incluye a los sistemas implicados en el tratamiento de la información dentro de la organización.

La información es un activo fundamental y cumple un rol vital en una empresa. Es como el oxígeno para el organismo: debe fluir adecuada y oportunamente por todas las áreas. También se deben evitar filtraciones hacia la competencia, entre otros riesgos. Precisamente, disponer de la certificación de un Sistema de Gestión de Seguridad de la Información (SGSI) ayuda a la organización a gestionar y proteger su información.

Estos son los principios:

Confidencialidad: mediante un SGSI se garantiza que la información de la organización no estará disponible ni será revelada a personas, organizaciones o procesos no autorizados.

Integridad: el SGSI promete mantener la información exacta y completa, tal como fue finalmente elaborada, así como sus métodos de proceso.

Disponibilidad: las personas, organizaciones y procesos que tengan acceso autorizado a la información deberán disponer de ella cuando la requieran.

Entre los beneficios que puede obtener una empresa que implemente un SGSI, tenemos: la disminución del impacto de los riesgos; mayores garantías de continuidad del negocio basadas en la adopción de un plan de contingencias; la mejora de la imagen de la organización y el aumento del valor comercial de la empresa y sus marcas; una mayor confianza por parte de clientes, proveedores, accionistas y socios; una mejora del retorno de las inversiones; el cumplimiento de la legislación y normativa vigentes, etc.

“En los casos de empresas internacionales o de aquellas que tengan proyectado internacionalizarse, se debe tener en cuenta que todos los sistemas de gestión basados en las normas ISO 27001:2013 son integrables entre sí, ya que contienen partes comunes que se pueden realizar y documentar a la vez, lo que facilita su implantación.” (educativa, 2018)

2.3 Marco conceptual

A continuación, veremos los conceptos que sustentan la construcción del mejoramiento para el fortalecimiento de la confidencialidad de la información:

Seguridad De La Información: “Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.” (Wikipedia, Seguridad de la información, 2010)

RIESGOS: “En arquitectura de computadores, un riesgo es un problema potencial que puede ocurrir en un procesador segmentado. Típicamente los riesgos se clasifican en tres tipos: riesgos de datos, riesgos de salto o de control y riesgos estructurales.” (Wikipedia, 2018)

Las instrucciones de un procesador segmentado son ejecutadas en varias etapas, de modo que en un momento dado se encuentran en proceso varias instrucciones, y puede que éstas no sean completadas en el orden deseado.

Un riesgo aparece cuando dos o más de estas instrucciones simultáneas (posiblemente fuera de orden) entran en conflicto.

ADWARE: “Es un programa de internet que cuando se ejecuta, muestra publicidad de internet y la descarga. El principal síntoma de infección de adware es la aparición de ventanas emergentes en nuestra computadora.” (Wikipedia, 2018)

Confidencialidad: Hablamos de confidencialidad cuando no referimos a la característica que asegura que los usuarios sean (personas, procesos, etc.), no tengan acceso a los datos a menos que estén autorizados para ello.

Disponibilidad: Garantiza que los recursos de sistema y la información estén disponibles solo para usuarios autorizados en el momento en que los soliciten.

Integridad: Nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos también autorizados.

Spyware: Es un programa espía que se instala sin autorización del cliente, y su objetivo es conocer los hábitos informáticos del usuario de la computadora. Esta información es enviada vía e-mail por empresas publicitarias. Se transmiten a través de adjuntos de correo electrónicos y programas descargados de sitios no confiables.

ISO: International Standards Organization. Una de las organizaciones de normalización más importantes. El gobierno de cada país está representado individualmente.

2.4 Marco legal

El proyecto es fundamentado en estos decretos y leyes que de acuerdo con la constitución colombiana respalda la confidencialidad de datos personales.

Constitución política de colombia:

Resolución 0002007 25 de julio del 2018 del ministerio de tecnologías de la información y las comunicaciones, en ejercicio de sus facultades legales y reglamentarias en especial la que le confiere el Decreto 1414 de 2017, y en desarrollo de lo dispuesto en el artículo 17 de la ley de 1581 de 2012 y en el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015 y considerando que la protección de los datos personales está consagrada en el artículo 15 de la Constitución Política como el derecho fundamental que tiene todas las personas a conservar su intimidad personal y familiar y su buen nombre, los mismo que conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos y en archivos de las entidades públicas y privadas.

Artículo 17 de la ley estatutaria 1581 de 2012: Consagró la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho, de manera que incorporo los lineamientos necesarios para que los organismos públicos y privados identifiquen los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones en las cuales se deben recolectar

los datos personales que posteriormente serán vinculados con la administración de una base de datos. (politica, 1991)

Capítulo 1. DISPOSICIONES GENERALES

Artículo 1. Objeto. El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Artículo 2. Tratamiento de datos en el ámbito personal o doméstico. De conformidad con lo dispuesto en el literal a) del artículo 2 de la Ley 1581 de 2012, se exceptúan de la aplicación de dicha Ley y del presente Decreto, las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico. El ámbito personal o doméstico comprende 1377 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012" aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.

Artículo 3. Definiciones. Además de las definiciones establecidas en el artículo 3 de la Ley 1581 de 2012, para los efectos del presente Decreto se entenderá por:

1. Aviso de privacidad: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

2. Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público.

Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

3. Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquello~ que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

4. Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

5. Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (politica, 1991)

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. A continuación, los artículos de la ley:

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. (asesores, 2018, pág. 10)

Capítulo 3: Diseño metodológico

3.1 Tipo de investigación

El proyecto es de enfoque cualitativo, con una investigación de carácter exploratoria y descriptivo porque se muestra cuál es el proceso que se debe tener para el diseño de un plan de mejoramiento para fortalecer la confidencialidad de la información de la empresa, y se llevara a cabo bajo 6 tipos de metodologías:

• Observación:

Inicialmente realizaremos visitas a la empresa con el fin de ver su proceso en un día normal de labores, sus métodos de trabajo, vehículos disponibles, procesamiento de información. Al igual observaremos si la información recolectada mediante el sistema está en óptimas condiciones y si cuenta con un sistema de protección.

• Recolección:

Se recolectará la información primaria relacionada con datos de la empresa, en cuanto a su proceso de recolección de datos de empleados y clientes, haciendo entrevistas a todos los colaboradores de la empresa. Me facilitaron el acceso a la información y me brindaron un contexto general de sus labores diarias y los problemas que se le presentan para la protección de datos.

• Análisis:

Al tener identificados claramente los puntos de vista, se procedió a la manipulación, procesamiento, análisis, tabulación e interpretación de resultados de la información, para obtener el diagnostico concreto de la situación de la empresa, y sus necesidades de mejoramiento.

• Diagnóstico:

Se evidencian las diferentes fallas del proceso, se ordenan por nivel de importancia, se identifican sus causas, y establece el orden a seguir para iniciar con el plan de acción correctivo y mejora del proceso.

• Desarrollo:

Se procederá a investigar las diferentes herramientas, que, para el campo de confidencialidad de la información, pueden ser aplicables, llegando a contemplar herramientas de informática ya existentes en el mercado, como app y programas que pueden tener una mayor seguridad a la hora de proteger la información.

• Conclusión:

Por último, se elaborará una propuesta con las posibles soluciones, para ser evaluadas por los directivos de la compañía, y tomar la decisión de desarrollarlas y llegar a ser implementadas.

3.2 Población

Tomaremos al personal administrativo que está conformado por el gerente, secretaria general, ingeniero de sistema, ingeniero ambiental, administrador de empresas y contador, para determinar la función del proyecto, y así tener una buena información.

3.3 Técnica e Instrumento de recolección de información

Las técnicas de recolección de datos que serán aplicadas en este proyecto son: La observación estructurada y las entrevistas. Mediante el análisis de observación estructurada se obtendrá información sobre lo que ocurre en la empresa en el manejo de la información y la seguridad de la misma, se tomaran datos sobre los problemas e inquietudes que presentan tanto el personal administrativo como técnicos e ingenieros; en relación con la técnica de la entrevista; se realizara directamente en el área administrativa y a los técnicos e ingenieros donde se recogerá gran cantidad de información, se desarrollan una serie de preguntas al personal donde se obtendrá información importante para el avance del proyecto.

3.4 Análisis de información

Mediante las actividades trazadas, como las entrevistas, se realizará un análisis detallado de la información recolectada en términos precisos donde se pueda observar la manera en cómo se maneja la información dentro de la empresa ECORED S.A.S y la seguridad de la misma, los

objetivos principales para desarrollar la investigación son: La observación, recolección y el análisis.

Para la selección de la herramienta informática que permita proteger la información de la empresa, nos reuniremos con los directivos y así evaluar que herramienta es la mejor y más eficaz que garantice la seguridad de la información y que beneficie a la empresa y sus clientes.

Capítulo 4. Presentación de Resultados.

Proteger los datos confidenciales es uno de los aspectos más importantes de salva guardar de una empresa. Estos bienes son relativamente importantes, para ello se necesita de una metodología que permita evaluar los controles y programas de una empresa, con el fin de actuar de manera necesaria y así disminuir los riesgos a los que se exponen tan solo por el hecho de existir.

Toda organización necesita auditorías que fortalezca los controles y acciones necesarias para mitigar el riesgo de pérdida o robo de información confidencial.

Tomando como referencia los objetivos propuestos desde el principio de nuestro proyecto de grado, se ha cumplido con todas las actividades programadas.

4.1 Fases del trabajo

El presente trabajo de investigación se desarrollará en las siguientes fases:

- Encuesta sobre el conocimiento de la regulación colombiana actual en cuanto a protección de datos personales.
- Análisis y elección de los datos a proteger de la empresa.
- Clasificación de los datos de la empresa, si serán de uso público, privado o confidencial.
- Se realizará una evaluación para ver que software es competente para la protección de datos confidenciales de la empresa ECORED S.A.S

- Presentación de resultados a los directivos de la empresa.

4.2 Diagnóstico

Para evitar el acceso a la información no autorizada, daños o intromisiones en los sistemas de la organización, se crean áreas seguras donde se definen:

- Perímetros de la seguridad informática.
- Controles físicos de entrada de información a los sistemas.
- Seguridad contra amenazas externas y del entorno

Estas pautas son necesarias para aplicar seguridad informática y modelos de trabajo en las áreas seguras.

Tomando esta serie de conceptos elaboramos una tabla con las situaciones encontradas en la organización ECORED S.A.S

Tabla 1. **DOFA**

DEBILIDADES	FORTALEZAS
No se tiene un amplio conocimiento sobre la seguridad de la información.	Cuenta con el área de soporte técnico dentro de la empresa y no depende de terceros.
La empresa no cuenta con servidor alterno para guardar los backup`s realizados en caso de algún evento.	El área de TI tiene personal calificado
Los Backus no son revisados después de realizados.	El antivirus utilizado brinda una seguridad estable.
Falta capacitación con respecto a seguridad de la información.	El licenciamiento de la empresa ECORED S.A.S es legal.
OPORTUNIDADES	**AMENAZAS**
La empresa cuenta con el presupuesto para la compra e innovación de las herramientas para tener una mejor seguridad de la información.	Perdida de información por no revisar las copias de seguridad después de que se ejecuten.
Realizar capacitaciones constantemente al personal.	Afectación de las bases de datos por el ingreso a paginas no permitidas.
La organización cuenta con las personas comprometidas con este proyecto.	Perdida de datos confidenciales de los clientes.

4.3 Conocimiento de la protección de datos confidenciales de la empresa.

Realizando un análisis de las 20 encuestas realizadas al personal en el área de TI, se logra evidenciar que el 4% su conocimiento es excelente, el 23 % su conocimiento es bueno, el 19% no tiene conocimiento, el 18% su conocimiento es muy deficiente y el 37% su conocimiento es regular, se puede definir que la mayoría del personal esto es 37% que labora en el área de TI tiene unos niveles de conocimiento de la protección de datos confidenciales muy bajos, o no los tiene, es de suma importancia establecer tareas o actividades que conlleven a que el personal nivele los conocimientos de seguridad de datos confidenciales.

Tabla 2. **Conocimiento sobre la protección de datos confidenciales**

1. Conocimiento sobre la protección de datos confidenciales.	E	B	NT	D	R
¿Qué conocimiento posee en cuanto a la seguridad de datos confidenciales de una empresa?	2	6	0	7	5
¿Qué conocimiento tiene sobre las normas de seguridad informática?	1	6	6	0	7
¿Cuál es su conocimiento sobre las normas ISO 27001?	1	6	1	0	12
¿Qué nivel de conocimiento adquiere en las capacitaciones que realiza las empresas en cuanto a la seguridad informática?	0	4	0	0	16

¿Sabe usted hasta qué punto es legal el uso que le da la empresa a los datos confidenciales?	0	2	10	6	2
¿Los equipos de cómputo tiene licenciamiento vigente?	1	2	6	10	1
¿Verifica usted los parámetros establecidos para el ingreso al sistema?	0	6	3	2	9
	4%	**23%**	**19%**	**18%**	**37%**

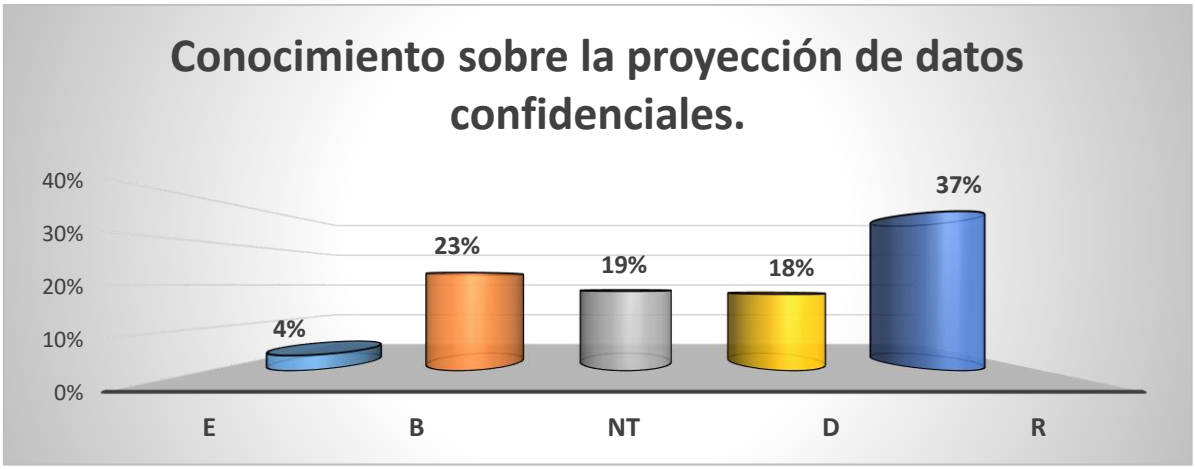

Figura 1. **Porcentaje conocimiento**

4.4 Análisis y elección de los datos a proteger de la empresa.

Después de haberse realizado una reunión con los directivos de la empresa, se llevó a cabo la categorización de información, las cuales estarán catalogadas bajo 3 conceptos: Uso público, uso privado y uso confidencial, adicional a ello se realiza una matriz de riesgo para evaluar así el impacto y la gravedad que pueden tener para la empresa en caso de sufrir alguna afectación.

Tabla 3. **Tabla 3: Publica, Privado y Confidencial**

PÚBLICO	PRIVADO	CONFIDENCIAL
➢ **Información fiscal de la empresa.** ➢ **Información laboral.** ➢ **Actividades de la organización.** ➢ **Marketing**	➢ Información administrativa. ➢ Toma de decisiones. ➢ Información de recursos humanos. ➢ Datos de los trabajadores de la empresa.	➢ Información financiera. ➢ Base de datos de los clientes. ➢ Archivos de la empresa. ➢ Información de colaboración empresarial.

MATRIZ DE RIESGOS

Datos a clasificar	Probabilidad (Ocurrencia	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
Archivos de la empresa.	4	5	20	Muy grave
Información financiera.	3	5	15	Muy grave
Base de datos de los clientes.	3	5	15	Muy grave
Información de colaboración empresarial.	2	5	10	Importante
Toma de decisiones	2	5	10	Importante
Datos de los trabajadores de la empresa.	2	5	10	Importante
Información administrativa	3	3	9	Importante
Información de recursos humanos.	1	5	5	Apreciable
Marketing	1	3	3	Apreciable
Información fiscal de la empresa.	1	2	2	Marginal
Información laboral.	1	2	2	Marginal
Actividades de la organización.	1	2	2	Marginal

Figura 2. Matriz de Riesgos

LEYENDA

			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Figura 3. Leyenda

4.5 Elaboración Del Plan Estratégico De Tecnologías De La Información Peti Ecored S.A.S

Introducción

El Plan Estratégico de Tecnología de ECORED S.A.S aparece como protección y disminución de la brecha digital para así garantizar el derecho a la información y a la comunicación, así mismo para la protección de dicha información, proporcionando la mejora continua en la gestión institucional. Aplicando estándares y prácticas en la implantación de sistemas informáticos.

Este plan se maneja en una serie de acciones encaminadas a optimizar los resultados que son producto de la gestión que la empresa ha ido manejando en los últimos años. ECORED S.A.S se ha preocupado de potenciar los deberes de los administrativos a través de la incorporación de estas tecnologías en sus procesos estratégicos, misionales y de apoyo.

Las normas expedidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones como también estándares internacionales como ITIL, COBIT, e ISO 27001, se encaminan en la aplicación de "buenas prácticas" y la prestación de servicios de TI con niveles de calidad, en condiciones seguras y siempre generando valor en el actuar organizacional.

4.5.1. Objetivo. Ordenar las estrategias para la dirección de las Tecnologías de la Información y las Comunicaciones TI en ECORED S.A.S, dependiendo de las necesidades de la empresa y los lineamientos.

- Fortalecer los softwares elegidos con un esquema de alta disponibilidad y seguridad.
- Desarrollar la automatización y eficiencia de los procesos soportados como la confidencialidad de datos.
- Incrementar la cobertura de los servicios de la oficina TI.
- Ejecutar las normativas que exigen.

.

4.5.2. Alcance

El Plan Estratégico aplica para todos los procesos que contribuyen al desarrollo de los recursos de tecnologías de información y comunicación en ECORED S.A.S.

La implementación de este PETI en la organización, llevara a cabo una eficiente apropiación de las tecnologías de la información, ganando ventajas como:

- Claridad sobre los elementos que orientaran las acciones de las tecnologías de información.

El PETI observa los lineamientos generados por el Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC en materia de Gobierno en línea y gestión estratégica de tecnologías de información. Principalmente lo contenido en el Marco de Referencia de Arquitectura Empresarial del Estado colombiano y en cada uno de sus dominios:

- Estrategia TI.
- Gobierno de TI.
- Información.
- Sistemas de información.
- Servicios tecnológicos.
- Uso y apropiación de TI.

4.5.3. Marco Legal

Tabla 4. Normatividad

NORMATIVA	DESCRIPCIÓN
Ley 1712 de 2014.	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Ley 1437 de 2011.	Código de Procedimiento Administrativo y de lo contencioso Administrativo.
Ley 1341 de 2009.	Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley 1266 de 2008.	Disposiciones generales de habeas data y se regula el manejo de la información.
Ley 962 de 2005.	Disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley 594 de 2000.	Dicta la Ley General de Archivos.
Ley 527 de 1999.	Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1757 de 2015.	Disposiciones en materia de promoción y protección del derecho a la participación democrática.
Artículo 17 de la ley estatutaria 1581 de 2012.	Consagró la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho, de manera que incorporo los lineamientos necesarios para que los organismos públicos y privados identifiquen los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones en las cuales se deben recolectar los datos personales que posteriormente serán vinculados con la administración de una base de datos. (política, 1991).

4.5.4. Análisis De La Situación Actual. Este análisis de la situación actual, tiene como base la información histórica de la empresa, la recolección de la información, la observación de los procesos y las necesidades establecidas.

Se agrupa la información y se presenta una breve descripción de los componentes identificados, en relación con los siguientes elementos:

SOFTWARE: es un término informático que hace referencia a un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas a un sistema informático. Tipos de software:

- Software de sistema.
- Software de programación.
- Software de aplicación.
- Software malicioso o mal intencionado.
- Software libre y software propietario.

SISTEMAS DE INFORMACIÓN: ECORED S.A.S cuenta con los siguientes sistemas de información.

- Facturación: Apoya los procesos misionales de la empresa, pues es donde se genera toda la facturación por el que hacer de la empresa.
- Formiik: Apoya el área financiera, contable y de presupuesto de la empresa.
- Bizneo: Apoya el área de gestión humana.

Es recomendable implementar mecanismos de control y auditorias para poder tener mayor seguridad de las acciones realizadas, sobre las bases de datos, contabilidad de la empresa, y accesos de información.

Se requiere un software lo bastante seguro y funcional para las necesidades de la empresa, y así soportar los procesos misionales con los niveles de oportunidad, disponibilidad, confiabilidad e integridad.

4.5.4.1 Estrategia de ti. ECORED S.A.S tiene su principal fortaleza en relación con la existencia de una oficina TI, esta oficina ha realizado avances en materia de alinear el PETI con los requerimientos del MINTIC

***4.5.4.2 Uso y apropiación de la tecnología*.** Se cuenta con un uso y apropiación de TI, esta oficina se encarga de divulgar y comunicar internamente y de forma constante los proyectos que se están implementado para conocimiento y apropiación por parte de los colaboradores de la empresa. Se han realizado capacitaciones respecto a las diversas soluciones.

***4.5.4.3 Gestión de información*.** La oficina identifica activos de información y a partir de los mismos participa constantemente en un ejercicio de coordinación interinstitucional con las entidades del sector para definir un modelo de protección de datos y de información que puedan verse en peligro de robos. Usa diferentes componentes de divulgación de información.

***4.5.4.4 TI*.** Se quiere implementar procesos de gestión que permitan administrar eficientemente los datos a proteger de la empresa, para ello se lleva a cabo el estudio de softwares para implementarlos en la empresa, 2 puntos clave de mayor importancia.

- Organizar, priorizar y brindar metodologías y control efectivo sobre la planeación y ejecución de dichos proyectos.
- Evaluación, y toma de decisiones de los proyectos.

***4.5.4.5 Analisis financiero*.** Se tiene un presupuesto distribuido en los siguientes frenes del área de informática y tecnología.

- Compra de los softwares.
- Cableado estructurado.
- Licenciamiento legal.
- Mantenimiento de aplicaciones.
- Mantenimiento de sistemas.
- Mantenimiento de equipos.

4.5.5 Entendimiento estrátegico

4.5.5.1 modelo operativo. El plan estratégico está fundamentado con los marcos estratégicos que tiene la empresa, como la misión, visión y valores de sí misma.

Misión

Somos una empresa ecológica de reciclaje y digitalización de archivos, comprometidas con el medio ambiente, que obtiene material reciclaje para su reutilización y producción de nuevos productos, organiza y digitaliza archivos a través de estrategias dirigidas a la comunidad y a los

grupos empresariales, generando conciencia con sobre la importancia de conservar el planeta, trabajando con amor y compromiso.

Visión

Ser en el 2018 una empresa líder en la recolección y producción de productos a partir de material reciclado, la digitalización de información y la reducción del papel con gran presencia a nivel local, nacional e internacional.

Valores

CONFIDENCIALIDAD: La reserva y confidencialidad de la información en el material reciclado es el principal objetivo con nuestros clientes.

HONESTIDAD: Actuando con honestidad hemos logrado construir la confianza de nuestros clientes, empleados y aliados, lo que nos permite garantizar la calidad en el cumplimiento de nuestros servicios.

AMOR: El amor por lo que hacemos y las ganas de contribuir con la creación perfecta de Dios nos lleva a trabajar juntos para lograr nuestros objetivos.

COMPROMISO: Orden, puntualidad y responsabilidad son características propias del compromiso de nuestro equipo con cada uno de nuestros clientes y proyectos.

***4.5.5.2 Necesidades De Información*.** Las necesidades de información de la empresa ECORED S.A.S se definen de la siguiente manera:

- Gestión financiera.
- Gestión de recursos humanos.
- Gestión documental.
- Gestión de facturación.
- Gestión comercial.

4.5.6. Modelo De Gestión De Ti. A continuación, se describe el modelo estratégico de gestión de tecnologías de información de ECORED S.A.S, el cual se continuará mejorando de forma continua durante los próximos años.

4.5.6.1 Estrategia Ti. La estrategia de TI en ECORED S.A.S está establecida en función de la protección de datos confidenciales de la empresa, a partir del acceso y uso de dicha información, con la planeación de una visión estratégica a ser desarrollada de inmediato teniendo claro que será requerida su actualización mensual. La estrategia se deriva bajo los siguientes principios:

- Contribuirá a la protección de los datos confidenciales.
- Permitirá contar con información oportuna y completa a los empleados de la organización.
- Facilitará y potenciará el trabajo de los colaboradores de la empresa, en cuanto a la protección de datos e información.

4.5.6.1.2 Alineación De La Estrategia Ti Con El Plan Estratégico Institucional

El plan estratégico se encuentra alineado al plan estratégico actual de la empresa, todas las actividades y proyectos desarrollados en el marco de su ejecución contribuirán al cumplimiento de los objetivos de ECORED S.A.S.

Tabla 5. Perspectivas estratégicas

PERSPECTIVAS ESTRATÉGICAS	OBJETIVOS ESTRATÉGICOS	OBJETIVOS DEL PETI
Protección de información y datos.	Mantener la confianza de los clientes, y colaboradores de la empresa.	Automatizar los procesos internos de la empresa, contando con programas que permitan el buen funcionamiento de los objetivos, como proteger información valiosa de ECORED S.A.S.
Procesos internos.	Incrementar la productividad y calidad en la prestación del servicio, amentar la calidad de los empleados para llevar a cabo una buena productividad.	Capacitar a los colaboradores de la empresa, para aumentar la calidad de lo que presta dicha organización, y ejecutar procesos de renovación.

Clientes y mercado.	Posicionar la marca ECORED S.A.S.	Proteger la base de dato de los clientes, para que la empresa tome credibilidad de mercado, con la implementación de esquemas de seguridad y control.

4.5.7. Plan De Comunicaciones Del Peti. Para llevar a cabo la apropiada implementación, uso y mejoramiento continuo en el marco del PETI, son necesarias acciones de divulgación e información de los alcances, actividades, informes, avances y documentación de transformaciones, gracias a las estrategias de TI en la empresa, por eso es necesario ordenar los canales de comunicación en torno a reportes de avance, y así involucrar a los miembros de la organización en las acciones.

4.6 Evaluación y elección de Software.

Para la empresa ECORED S.A.S la información y los datos de los clientes, empleados, y demás archivos es de suma importancia, porque un solo ataque significa pérdidas económicas y perdidas de credibilidad empresarial.

Escoger un software para la protección de datos confidenciales no siempre es tan fácil como parece, su elección depende de múltiples factores.

Nos reunimos con la oficina de TI y tuvimos en cuenta estos factores para la elección del software:

- Que se ajuste a la normativa que exige la superintendencia de industria y comercio.
- Tiempo de implementación.
- Proveedor del software.
- Cumplimiento de protocolos (ciberseguridad y calidad de procesos).
- Que el software tenga la capacidad de jerarquizar la información.

Nos vimos en la obligación de escoger dos softwares para la eliminación completa de riesgos, ya que anteriormente la empresa se vio afectada por algunos robos informáticos.

1. ACUNETIX: A parte de ser un software que escanea la vulnerabilidad web, también monitorea las aplicaciones online y así prevenir cualquier irrupción a los sistemas. Cuenta con rastreo automático, sistema de reportes destallados y cuenta con un interfaz amigable.

Fuente: acunetix.com

Figura 4. Acunetix. Fuente: Acunetix

2. DATA PROTECTED: Unos de los puntos por los cuales hay que hacerle relevancia a este software es porque cuenta con las normativas exigidas por la superintendencia de industria y comercio, lleva el cumplimiento de la ley 1581 de protección de datos, y está muy comprometida con las empresas.

Fuente: DATAPROTECTED.COM.CO

Figura 5. Dataprotected. Fuente: Dataprotected.com.co

Capítulo 5. Conclusiones.

El objetivo de este trabajo de grado era diseñar un plan de mejoramiento para garantizar la confidencialidad de la información de la empresa ECORED S.A.S. Después de los análisis que permitieron la evaluación del estado actual de la protección de datos confidenciales la información arrojada es la falta de conocimiento por parte del personal de la organización, así mismo se permitió identificar las estrategias para desarrollar paso a paso el cumplimiento de los objetivos.

La aplicación de la estrategia y el monitoreo constante de las labores y responsabilidades asignadas a cada uno de los integrantes, permitirán identificar los riesgos a los que están expuestos dentro de la organización, así mismo atacarlos y realizar las correcciones pertinentes con el fin de hacer mejoras continuas y proteger la información para que no se vea afectada la empresa

Capítulo 5. Recomendaciones

Efectuar Auditorias Técnicas A nivel de: Software, Redes y Equipos de Comunicación utilizando metodologías de auditorías técnicas de seguridad.

Se debe realizar un cronograma de capacitación en temas de seguridad informática con la finalidad de que todo el personal que labora en ECORED tenga el conocimiento adecuado para el manejo de la información que se maneja en la compañía.

Formar un comité entre directivos y personal del Área de TI con el fin de evaluar los eventos que se registren en los softwares recomendados para definir estrategias de cómo proceder al respecto de cada evento que se presente.

Referencias

Asesores, D. (2018). Articulos . En D. Asesores. Bogota.

Digital, C. (2010). Protección De Información .

ECORED , S. (2006). *Reseña De La Empresa* . Valledupar: Publicaciones De Marketing.

Educativa, E. (2018). Importancia Y Beneficios De Contar Con Un Sistema De Gestion De Seguridad De Información. *Apuntes*.

Interior, M. D. (S.F.). Normas .

Politica, C. (1991). Leyes.

Portafolio. (2017). *Servicios* . Colombia.

Sapsi. (2003). Seguridad Informatica. Colombia : 4.

Wikipedia. (2000). Reseña Historica De Valledupar . *Valledupar* , 1.

Wikipedia. (2010). Seguridad De La Información. 5.

Wikipedia. (2018).

Wikipedia. (2019). *Valledupar* .

Apéndices

Apéndice A

Encuestas:

A continuación, veras unas preguntas las cuales debes leer y responder con una X según tu conocimiento.

1. ¿Qué conocimiento posee en cuanto a la seguridad de datos confidenciales de una empresa?

Excelente _____

Bueno _____

No tiene conocimiento _____

Deficiente _____

Regular _____

2. ¿Qué conocimiento tiene sobre las normas de seguridad informática?

Excelente _____

Bueno _____

No tiene conocimiento _____

Deficiente _____

Regular _____

4. ¿Qué nivel de conocimiento adquiere en las capacitaciones que realiza las empresas en cuanto a la seguridad informática?

Excelente _____

Bueno _____

No tiene conocimiento _____

Deficiente _____

Regular _____

5. ¿Sabe usted hasta qué punto es legal el uso que le da la empresa a los datos confidenciales?

Excelente _____

Bueno _____

No tiene conocimiento _____

Deficiente _____

Regular _____

6. ¿Los equipos de cómputo tiene licenciamiento vigente?

Excelente _____

Bueno _____

No tiene conocimiento _____

Deficiente _____

Regular

Apéndice B